(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開平７－６４９１１

(43)公開日　平成7年(1995)3月10日

(51)Int. Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ａ	7459－５Ｌ		
19/00				
			Ｇ０６Ｆ　15/30　３３０	

審査請求　未請求　請求項の数３　ＯＬ　（全１２頁）

(21)出願番号　特願平５－２１６０５６

(22)出願日　平成5年(1993)8月31日

(71)出願人　000005049
シャープ株式会社
大阪府大阪市阿倍野区長池町22番22号

(72)発明者　榎本　好晴
大阪府大阪市阿倍野区長池町22番22号　シャープ株式会社内

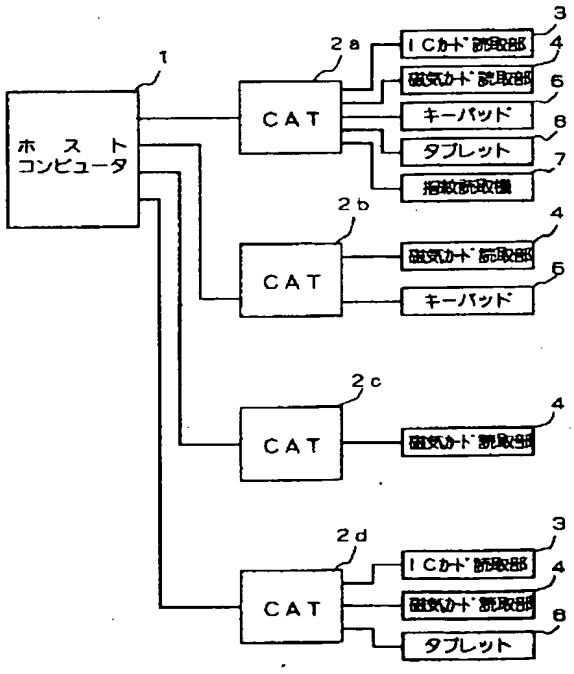
(74)代理人　弁理士　小森　久夫

(54)【発明の名称】個人認証システム

(57)【要約】

【目的】システムの各部で必要に応じてチェックの信頼度を向上させるようにして、必要十分なチェックを行うことができるようにする。

【構成】ＣＡＴ端末２ａ，２ｂ・・・のそれぞれに必要に応じてパスワード照合用のキーパッド５、サイン照合用のタブレット６、指紋照合用の指紋読取装置７を接続して、ＣＡＴ端末の設置場所に応じて必要十分な個人認証機能を備えるとともに、多くの機能を備えたＣＡＴ端末（例えば２ａ）でもその場面場面で必要な機能だけを用いて個人認証を行う。



1

【特許請求の範囲】

【請求項１】パスワード、筆跡、指紋等の個人を識別するための個人認証データの中から任意項目数の個人認証データを登録する個人データ登録手段と、各項目ごとの個人認証データを入力する入力装置の中から任意数の入力装置を選択的に接続する入力装置選択手段と、前記入力装置から入力された個人認証データと前記個人データ登録手段に登録された個人認証データとを照合する照合手段と、を備えたことを特徴とする個人認証システム。

【請求項２】請求項１に記載の個人認証システムにおいて、

前記照合手段により照合を行う項目を選択設定する照合項目選択手段を備えたことを特徴とする個人認証システム。

【請求項３】請求項２に記載の個人認証システムにおいて、

選択された照合を行う項目が使用不可状態であるとき、他の項目を代用する手段を備えたことを特徴とする個人認証システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】この発明は、個人の正当性確認および本人確認を実施する個人認証システムに関し、例えば、クレジット処理、キャッシング処理等の金融取引時の個人認証や、企業内等での入退室チェック時の個人認証に用いられる。

【０００２】

【従来の技術】従来の金融取引装置や入退室チェック装置における個人認証には次のような方法および装置が用いられていた。

【０００３】①　例えば、クレジットカードにおける個人認証の場合、クレジットカードの利用者のサインを店員等のサービス提供者が目視で確認する方法で、カード上のエンボス文字をインプリントした取引証書にカード利用者がサインして、その筆跡を店員等のサービス提供者が目視で確認する方法。

【０００４】②　同じくクレジットカードにおける個人認証の場合で、ＣＡＴ端末を利用し、パスワード入力用ピンパッド（通常、暗証番号の入力用としてテンキーパッドを用いる）からパスワードを入力し、それを照合する。パスワード（暗証番号）を入力し照合する方法は、銀行でのキャッシュカードによる個人認証にも用いられている。このパスワードの照合は、パスワードをカードの磁気ストライプに記しておいて端末自身がそのパスワードを読み取り照合を行う場合と、パスワードをホストが記憶しておいて回線を介して送受信を行いホスト側で照合を行う場合とがある。

【０００５】③　また企業内等での入退室許可のための個人認証においても、カード上に磁気ストライプで記載されたデータを読み取る装置、キーボードから入力されるパスワードを照合する装置、指紋入力部から入力される指紋等を照合する装置等が用いられ個人認証を行う。

2

【０００６】

【発明が解決しようとする課題】ところが上記した従来の構成では次のような問題があった。

【０００７】①　店員等のサービス提供者自身が目視でサインの照合を行う方法の場合、サインの照合には熟練が必要であり、実際のサービス提供者の数はサインの照合に熟練した者の数に到底及ぶものではないことから、盗難カード等でサインが偽造された場合のチェックはほぼ素通りの状態にある。

【０００８】②　ピンパッドからパスワードを入力して照合する方法では、パスワードの盗難が発生することがある。すなわち、近年では磁気的に記したパスワードを読み取ることが可能になっておりカードの磁気ストライプにパスワードを記した場合にはその盗難が比較的容易である。またパスワードとしては一般に暗証番号が用いられることが多いが、カード利用者が暗証番号を設定する場合には、生年月日等のカード利用者にとって記憶し易い番号を設定することが多く、それらのデータの盗難も比較的容易であることから、暗証番号の盗難が発生することがある。

【０００９】上記したように、従来金融取引に用いられていた個人認証のシステムは比較的簡易な構成であるために不正が発生し易い。金融取引額が大きい場合にこのような不正が発生すると損害は多大なものとなる。

【００１０】これを防止するために、例えば、特開昭５９－４３４７３号公報、特開平３－２６５０８６号公報に示されるように、暗証番号の照合の他に指紋照合，音声照合等の複数のチェック項目を組み合わせてチェックシステムを構築することも考えられるが、その場合には各端末に、暗証番号の入力部、指紋の入力部、音声の入力部等複数の入力部や照合部等を設ける必要があり、システムが高価になってしまう。金融取引額が大きい場合には高価なシステムを用いる価値はあるが、小額の取り引きしか行わない場合でも高価なシステムを備えるのは無駄であり、また、小額の取り引きの場合に過大なチェックを行うことは顧客に対して不快なイメージを与えるばかりでなく、時間のロスが多くなってしまう。

【００１１】一方、③に示した企業内等で入退室チェック等に用いられる個人認証システムでは、磁気ストライプを読み取る装置、パスワードを照合する装置、指紋を照合する装置等、いずれの装置を用いた場合でも、単独のチェックシステムである限りセキュリティ性の信頼度を向上させるには限界があった。

【００１２】この発明の目的は、システムの各部で必要に応じてチェックの信頼度を向上させるようにして、必要十分なチェックを行うことができる個人認証システムを提供することにある。

【００１３】

【課題を解決するための手段】請求項１に記載した発明は、パスワード、筆跡、指紋等の個人を識別するための個人認証データの中から任意項目数の個人認証データを登録する個人データ登録手段と、各項目ごとの個人認証データを入力する入力装置の中から任意数の入力装置を選択的に接続する入力装置選択手段と、前記入力装置から入力された個人認証データと前記個人データ登録手段に登録された個人認証データとを照合する照合手段と、を備えたことを特徴とする。

【００１４】請求項２に記載した発明は、請求項１に記載のシステムにおいて、前記照合手段により照合を行う項目を選択設定する照合項目選択手段を備えたことを特徴とする。

【００１５】請求項３に記載した発明は、請求項２に記載の個人認証システムにおいて、選択された照合を行う項目が使用不可状態であるとき、他の項目を代用する手段を備えたことを特徴とする。

【００１６】

【作用】請求項１に記載した発明においては、パスワード，筆跡，指紋等の個人を識別するための複数の項目のうちから必要な項目のみを選択してシステムを構築することができる。すなわち、入力装置選択手段により、必要な項目の入力装置のみを接続すれば不必要な入力装置を接続する無駄がなくなり、また、個人データ登録手段により必要な項目の個人認証データのみを登録すれば不必要なて登録の無駄がなくなる。そして適宜登録された個人認証データと、適宜選択接続された入力装置によって個人認証が行われる。

【００１７】請求項２に記載した発明においては、多数の個人認証データが登録されていたり、多数の入力装置が接続されている場合であっても、その中から任意の項目が選択されてデータの照合が行われる。したがって例えば、パスワード，筆跡，指紋の３項目の個人認証データの登録、およびこれらの項目の入力装置が接続されている場合であっても、それらの中から任意の項目、例えばパスワードのみを選択して照合を行うことができる。

【００１８】請求項３に記載した発明においては、例えば、選択された入力装置が故障している場合や、何らかの原因で使用可能状態が外れた状態である場合に他の項目が代用されて用いられるため、システムの動作が停止してしまうことがない。

【００１９】

【実施例】図１はこの発明の実施例に係る個人認証システムの構成例を示す図である。

【００２０】ホストコンピュータ１には複数のＣＡＴ端末２ａ，２ｂ・・・が接続されている。各ＣＡＴ端末２ａ，２ｂ・・・には個人認証データを入力装置として、ＩＣカードを挿入してその読み取りを行うためのＩＣカード読取部３、磁気カードのデータの読み取りを行う磁気カード読取部４が必要に応じて備えられるとともに、

パスワード入力用のキー（通常は、暗証番号を入力するためのテンキー）を有するキーパッド（ピンパッド）５、サイン入力用のタブレット６、指紋入力用の指紋読取装置７が必要に応じて接続されている。なお入力装置は個人を認証するためのデータが入力できるものであればよく、他に、声紋をチェックするための音声入力装置等が接続可能である。

【００２１】ＩＣカード読取部３、磁気カード読取部４に挿入されるＩＣカード、磁気カードにはそれぞれ個人を認証するための個人認証データや識別番号等の個人データが記憶されている。ＩＣカードには識別番号、有効期限、パスワード等の通常のデータの他に、サイン（筆跡）、指紋等の高度な個人認証データも記憶されている。また磁気カードには通常のデータ、すなわち識別番号，有効期限や、パスワード等の簡単な個人認証データが記憶されている。したがって、ＩＣカードを所有している個人に対しては識別番号，パスワードによるチェックの他に、サインや指紋の照合によるチェックも行うことができ、個人認識の確実性が向上する。

【００２２】しかし、ＩＣカードはそれだけで高価であるばかりでなく、サイン，指紋の照合を行うためにはそれらの入力装置，照合装置が必要であり、コスト高になる。一方、磁気カードを所有している個人に対しては識別番号，パスワードのチェックや目視によるサイン確認を行えるだけであるので個人認識の確実性はあまり高くはないが、コスト的には安価な構成となる。

【００２３】個人は必要に応じてＩＣカードまたは磁気カードのいずれかを所有することになるが、コストとの兼ね合いから、高度なセキュリティ性が要求される場合にはＩＣカード、普通程度のセキュリティ性が必要な場合には磁気カードが用いられる。例えば、カードがクレジットカード等の金融取引カードである場合には、高額の取り引きを行う可能性がある顧客はＩＣカードを所持し、所定金額以下の取り引きのみの場合には磁気カードを所有することが考えられる。また企業内等での入退室チェックの場合には、重要度の高い部屋への入退室を行う者についてはＩＣカードを所有し、通常の部屋への入退室を行う者については磁気カードを所有することが考えられる。

【００２４】なおこの実施例では個人認証データをＩＣカード，磁気カード内に記憶しているが、ＣＡＴ端末２に記憶したり、ホストコンピュータ１に記憶しておいてもよい。ホストコンピュータ１に記憶した場合には、照合時にＣＡＴ端末２とホストコンピュータ１とが通信を行うことで照合を実行する。すなわち、上記の例では個人データ登録手段をＩＣカードや磁気カードが有しているが、該個人データ登録手段をＣＡＴ端末２やホストコンピュータが備えていてもよい。

【００２５】前記したように、ＣＡＴ端末２ａ，２ｂ・・・のそれぞれは必要に応じてＩＣカード読取部３、磁

気カード読取部４、キーパッド５、タブレット６、指紋読取装置７等のデータ入力部を有している。図２はＣＡＴ端末の構成例を示す図、図３はＣＡＴ端末のブロック図である。

【００２６】ＣＡＴ端末２にはＩＣカード読取部３、磁気カード読取部４、キーパッド５、タブレット６、指紋読取装置７等の入力装置がそれぞれスイッチＳＷ１～ＳＷ５、コネクタ２５ａ～２５ｅを介して接続可能になっている。したがって必要な入力装置のみをコネクタ２５ａ～２５ｅを用いて接続することができる。例えば、金融取引システムの場合、接続する入力装置をそのＣＡＴ端末で取り扱う金額に応じて設定することができ、例えば、ごく小額の取り引きのみを行う端末の場合には簡易チェックを行うために、磁気カード読取部４のみを備えていても良いし、キーパッド５等も追加して備えてもよい。また、高額の取引を行う可能性のある端末の場合にはより高度なチェックを行うために、ＩＣカード読取部３、および個人認証の確実性の高いサイン照合用のタブレット６や、指紋照合用の指紋読取装置７が追加してもよい。企業内等での入退室チェックを行うシステムの場合も同様で、簡易チェックで良い場合にはパスワード入力のためのキーパッド５のみ、磁気カード読取部４のみ、としたり、これらを組み合わせてみてもよいし、高度なセキュリティ性を要する場合にはＩＣカード読取部３と、サインや指紋の照合を行うためのタブレット６や指紋読取装置７を備えてもよい。ただし、サイン入力用のタブレット６、指紋入力用の指紋読取装置７を接続する場合で、ＩＣカード内にサインや指紋の個人データを記憶した場合にはＩＣカード読取部４は必須となる。

【００２７】また、コネクタにより接続した入力装置でもスイッチＳＷ１～ＳＷ５をオン／オフすることによって接続状態を有効／無効にすることができる。このスイッチＳＷ１～ＳＷ５は、例えば、入力装置のいずれかが故障した場合にその装置をオフしたり、例えばいずれかの入力装置を用いた方法で不正が発生してその装置による照合を停止する場合にオフしたりする場合に用いられる。コネクタ２５ａ～２５ｅ、スイッチＳＷ１～ＳＷ５が請求項１に記載した入力装置選択手段に対応する。

【００２８】このように必要に応じてＣＡＴ端末ごとにデータ入力部を適宜設定できるため、例えば小額の取り引きしか行わない端末に、ＩＣカード読取部３やタブレット６、指紋読取装置７等の高価な装置を備える必要がなく、システムが必要以上に高価になってしまうのを防止することができる。またパスワード、磁気カード、ＩＣカードのいずれを用いても個人チェックが可能なようにしているため、例えば小額の取り引きしか行わない顧客に対しては磁気カードを発行して、高価なＩＣカードの使用を避けることができる。

【００２９】ＣＡＴ端末２は、ＣＡＴ端末および該ＣＡＴ端末に接続された各入力装置の処理動作を制御するＣ

ＰＵ２１、処理プログラムを記憶するＲＯＭ２２、各入力装置の選択条件等を記憶するＲＡＭ２３、前記各入力装置の選択条件を入力するための選択条件入力設定部２４、ホストコンピュータ１との通信を行うためのモデム２６や、ディスプレイ１０、取引金額等の入力を行うためのキーパネル１１を有している。選択条件入力設定部２４、および、ＲＡＭ２３の選択条件の記憶部が請求項２に記載の照合項目選択手段に対応する。

【００３０】選択条件入力設定部２４は例えば端末の設置時や、必要に応じたメンテナンス時等に入力装置の選択条件を入力する部分である。例えば、金融取引装置では入力された金額ごとに個人認証方法が設定されて入力されたり、ＣＡＴ端末を設置した場所に応じて個人認証方法が設定されて入力される。また例えば、入退室チェックの場合には重要度に応じて個人認証方法が設定される。なおこの入力時、同時に、選択条件入力設定部２４からは、各入力装置の代用順も入力される。例えばＩＣカード読取部が使用不可な状態のときには磁気カード読取部が代用される、というように代用する認証方法が入力される。そして設定された選択条件に応じて個人認証処理が実行される。

【００３１】このシステムの動作手順を説明する。図４～図９はその処理手順を示すフローチャートであり、金融取引において取引金額高に応じて個人認証方法を選択するように選択条件入力設定部２４から入力された場合の状態を示している。

【００３２】まず、ＣＡＴ端末２の電源がオンされると初期化処理を行い、それとともに接続されている各入力装置が使用可能であるかどうかを検証する（ｎ５１→ｎ５２）。そして異常がなければ入力待ち状態へと進むが、使用不可能な装置がある場合には、例えば『○○が使用不可能です』を表示する等の警告動作を行い、続行を示す入力がされるまで、所定時間待機する（ｎ５３→ｎ５４→ｎ５５→ｎ５６）。もし、所定時間内に続行を示す入力がされなかった場合にはそのままエラー処理となるが、続行が入力がされた場合には該当する部分の入力装置を代用させて設定する（ｎ５７）。例えば、いま、選択条件入力設定部２４から入力された条件が、小額取引の場合にはパスワード照合のみを行うことであるとする。ところが入力装置としてパスワードの入力装置（キーパッド５）が使用不可能であるとすると、予め選択条件入力設定部２４から入力されているデータに基づいてパスワードの入力装置の他のものに代用させる。例えば、代用としてサインの照合が設定されている場合にはパスワードに代えてサインの照合を設定し、この条件を該ＣＡＴ端末２の電源オフまでの間選択条件として記憶する。このようにし代用設定された装置について上記と同様に検証を行い、異常がなければ入力待ち状態になる（ｎ５８→ｎ５９→ｎ６０）。

【００３３】次に取引処理時の手順を説明する。

【００３４】まず取引の前処理として、取り引きの種類，金額等の入力を行う（ｎ１）。種類は例えば、クレジットの場合であると『売上げ』等であり、銀行のカードであると『引出し』等である。そしてカード（磁気カードまたはＩＣカード）が挿入されると、そのカードに記載されている識別番号，有効期限等を読み取って、該ＣＡＴ端末での使用の可否のチェック、有効期限チェック、ネガチェック、預信限度額のチェック等を行う（ｎ２→ｎ３）。通常、ＣＡＴ端末での使用の可否チェック，有効期限チェック等の簡単なチェックはＣＡＴ端末自身で行うが、他のネガチェック，予信限度額チェック等の複雑なチェックはホストコンピュータ１へ識別番号を送信して、ホストコンピュータ１側で行われる。チェック結果が正常な場合には、照合項目の設定処理へと進むが、チェック結果に異常があった場合、例えば有効期限切れや予信限度額をオーバーしていた場合等には取り引きの解除処理を行う（ｎ４→ｎ６，ｎ５）。取引解除処理は、ＣＡＴ端末のディスプレイ１０にエラー表示を行うとともに、ＩＣカード９を取り込んでいた場合にはそのＩＣカードの非活性化処理および排出を行う。

【００３５】照合項目の設定処理は図６に示すように、ｎ１において入力された取引金額に応じて照合項目を選択設定する（ｎ２１→ｎ２２，ｎ２３，ｎ２４）。

【００３６】ｎ６で照合項目が設定されるとそれに応じてパスワード，サイン，指紋のそれぞれの照合をＣＡＴ端末内、ＩＣカード内、またはホストコンピュータ内で行う（ｎ８→ｎ９，ｎ１０→ｎ１１，ｎ１２→ｎ１３）。

【００３７】例えばパスワードの照合はＣＡＴ端末内で行う。パスワードの照合は図５に示すように、磁気カードまたはＩＣカードから読み込んだパスワードと、キーパッド５から入力されたパスワードとを照合し、両者が一致すればメインフローへと戻る（ｎ３１→ｎ３２→ｎ３３→ｎ３４）。一方、両者が一致しない場合には数回のリトライを行うが、それでも一致しない場合にはエラー処理として取引解除処理を行う（ｎ５）。このリトライ回数は、ＣＡＴ端末において適宜設定される。なお、磁気カード８やＩＣカード９にパスワードが記載されていない場合にもエラーを判定して取引解除となる（ｎ５）。この実施例ではパスワードの照合をＣＡＴ端末内で行っているが、パスワードを予めコストコンピュータ１内に記憶しておいて、ホストコンピュータ１内で照合を行ってもよく、また、ＩＣカードを用いる場合にはＩＣカード内で照合を行ってもよい。

【００３８】サインや指紋の照合はＩＣカード内で行われる。例えばサインの照合は図６に示すように、ＣＡＴ端末のタブレット６からサインが入力されると、ＩＣカード内で照合が行われる（ｎ４１→ｎ４２→ｎ４３→ｎ４４，ｎ４５→ｎ４６）。また指紋の照合も図７に示すように、ＣＡＴ端末の指紋読取装置７から指紋が入力されると、ＩＣカード内で指紋の照合が行われる。

【００３９】以上のような照合処理により個人の認証が行われた場合には取引を許可して取引許可処理を実行する（ｎ１４）。すなわち、取り引きのためのデータ処理を行い、その結果をホストコンピュータに送信したり、ＩＣカードに書き込んだ後、ＩＣカードの排出処理等を行う。

【００４０】以上のように必要に応じて適宜個人の照合項目が選択されて照合処理が行われる。これによって小額取引時等の高度な認証が不必要な場合等には簡易な認証のみを行うことができ、ランニングコストを安価にするとともにチェック時間も短縮でき、さらに、小額取引時等には指紋チェック等の顧客に対するイメージが悪い項目を削除することができ、顧客に対するサービス性の低下も防止できる。

【００４１】

【発明の効果】請求項１，２に示した発明によれば、必要に応じて照合項目を設定することが可能になるため、例えば簡易的な認証だけで良い場所や場面では簡易認証を行ってシステムコストまたはランニングコストを安価にすることができ、また例えば高度な認証を必要とする場所や場面では高度な認証を行ってセキュリティ性を向上させることができる。

【００４２】また請求項３に示した発明によれば、一つの照合項目が使用不可能な場合には他の項目で代用して照合が行われるため、システム自体がストップしてしまうことがない。

【図面の簡単な説明】

【図１】この発明の実施例である金融機関での個人認証システムの構成例を示すブロック図である。

【図２】同システムのＣＡＴ端末の構成例を示す図である。

【図３】同ＣＡＴ端末の要部ブロック図である。

【図４】同ＣＡＴ端末の動作開始時の処理手順を示すフローチャートである。

【図５】同システムにおける金融取引手順例を示すフローチャートである。

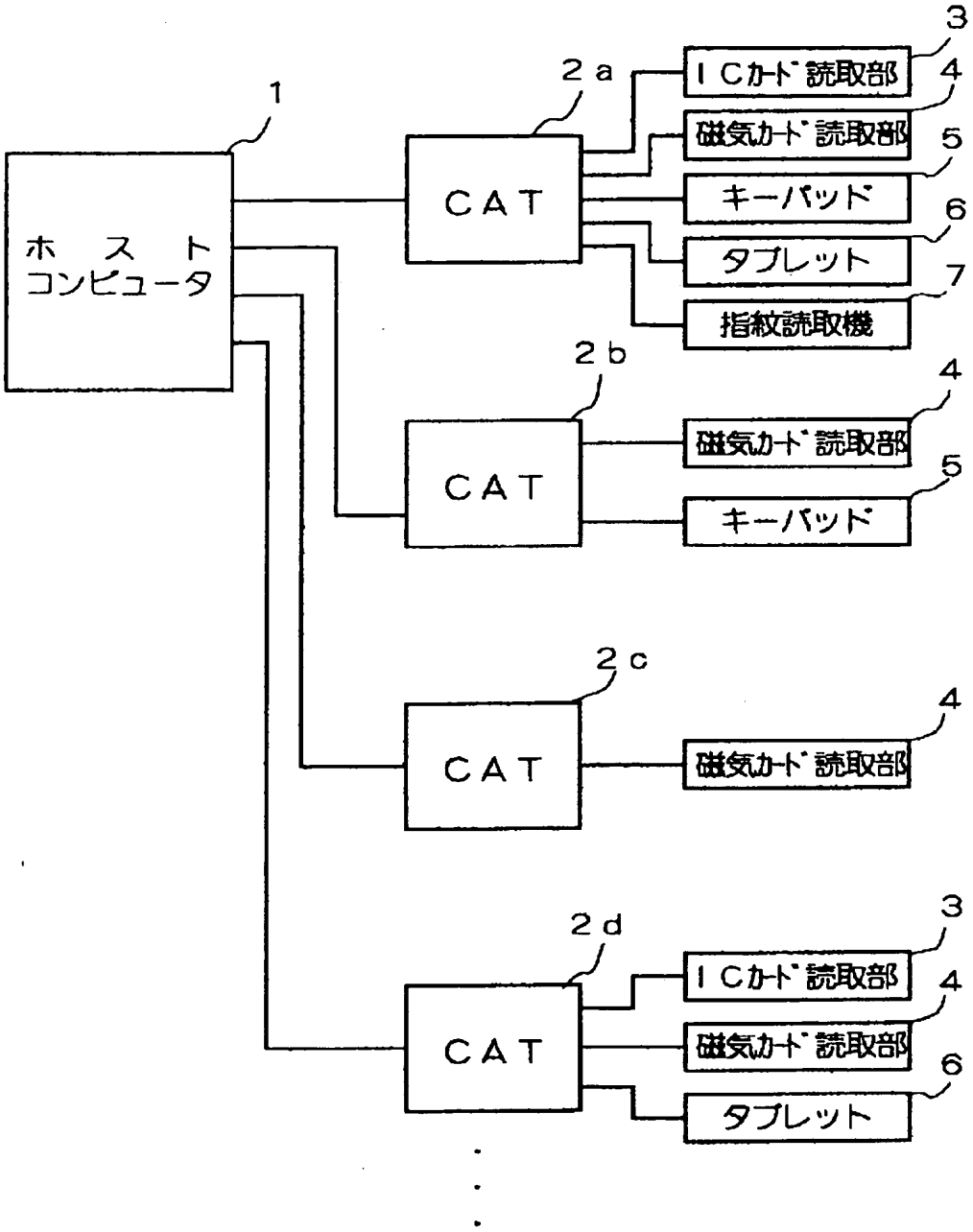
【図６】同システムにおける照合項目の設定手順例を示すフローチャートである。

【図７】同システムにおける個人認証の処理手順を示すフローチャートである。

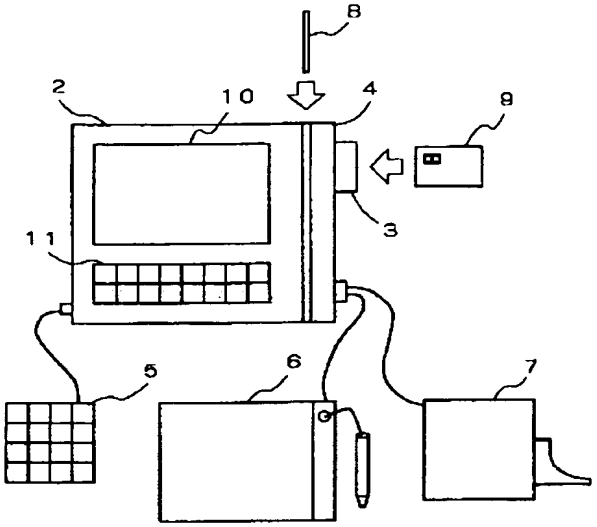
【図８】同システムにおける個人認証の処理手順を示すフローチャートである。

【図９】同システムにおける個人認証の処理手順を示すフローチャートである。

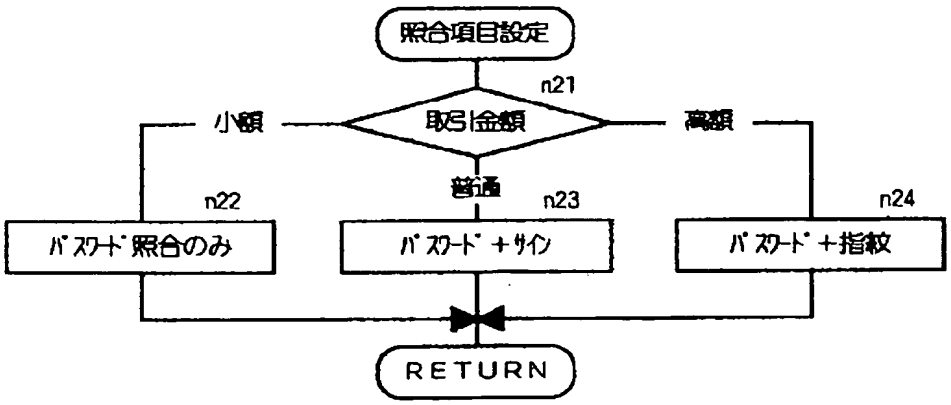
【図１】


ホスト
コンピュータ
1
CAT
2a
CAT
2b
CAT
2c
CAT
2d
ICカード読取部
磁気カード読取部
キーパッド
タブレット
指紋読取機
3
4
5
6
7

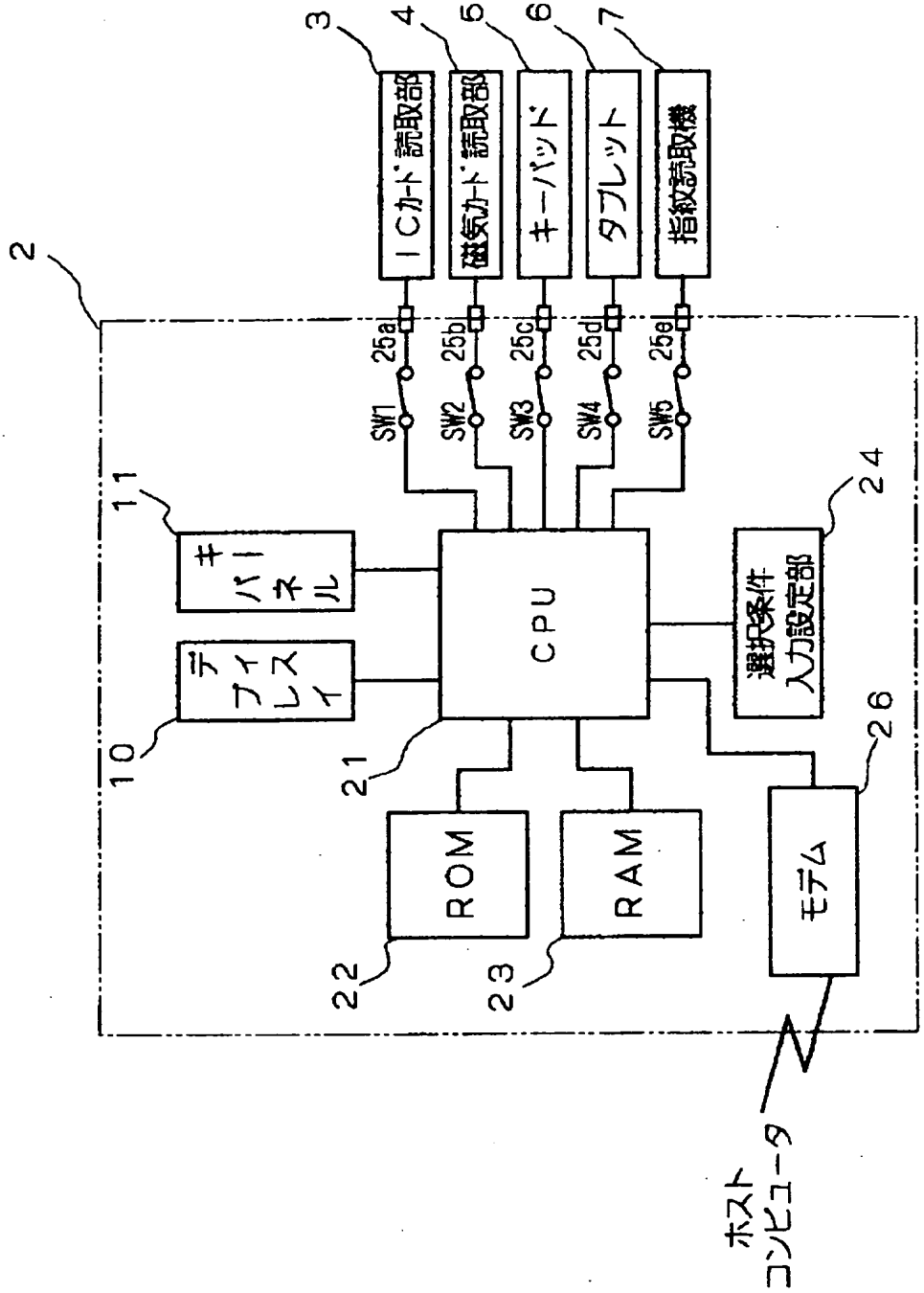
【図２】


8
2
10
4
9
3
11
5
6
7

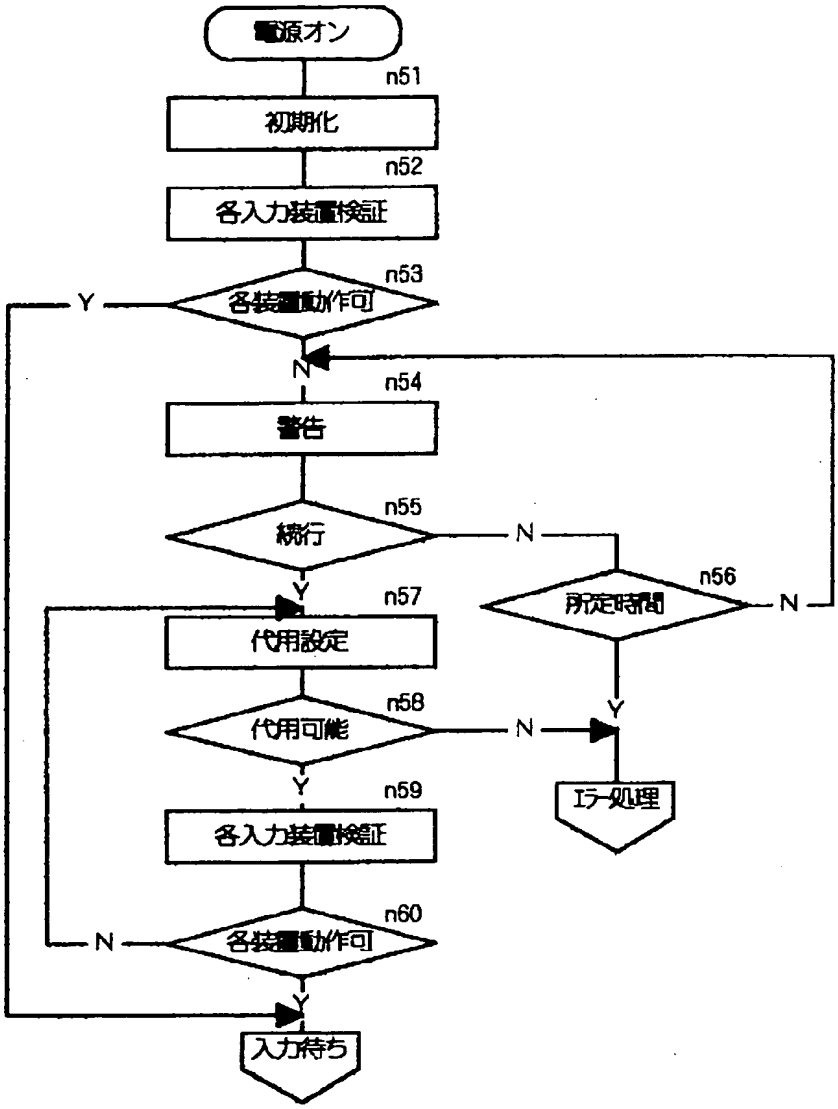
【図６】


照合項目設定
n21
小額
取引金額
高額
普通
n22
n23
n24
パスワード照合のみ
パスワード＋サイン
パスワード＋指紋
RETURN

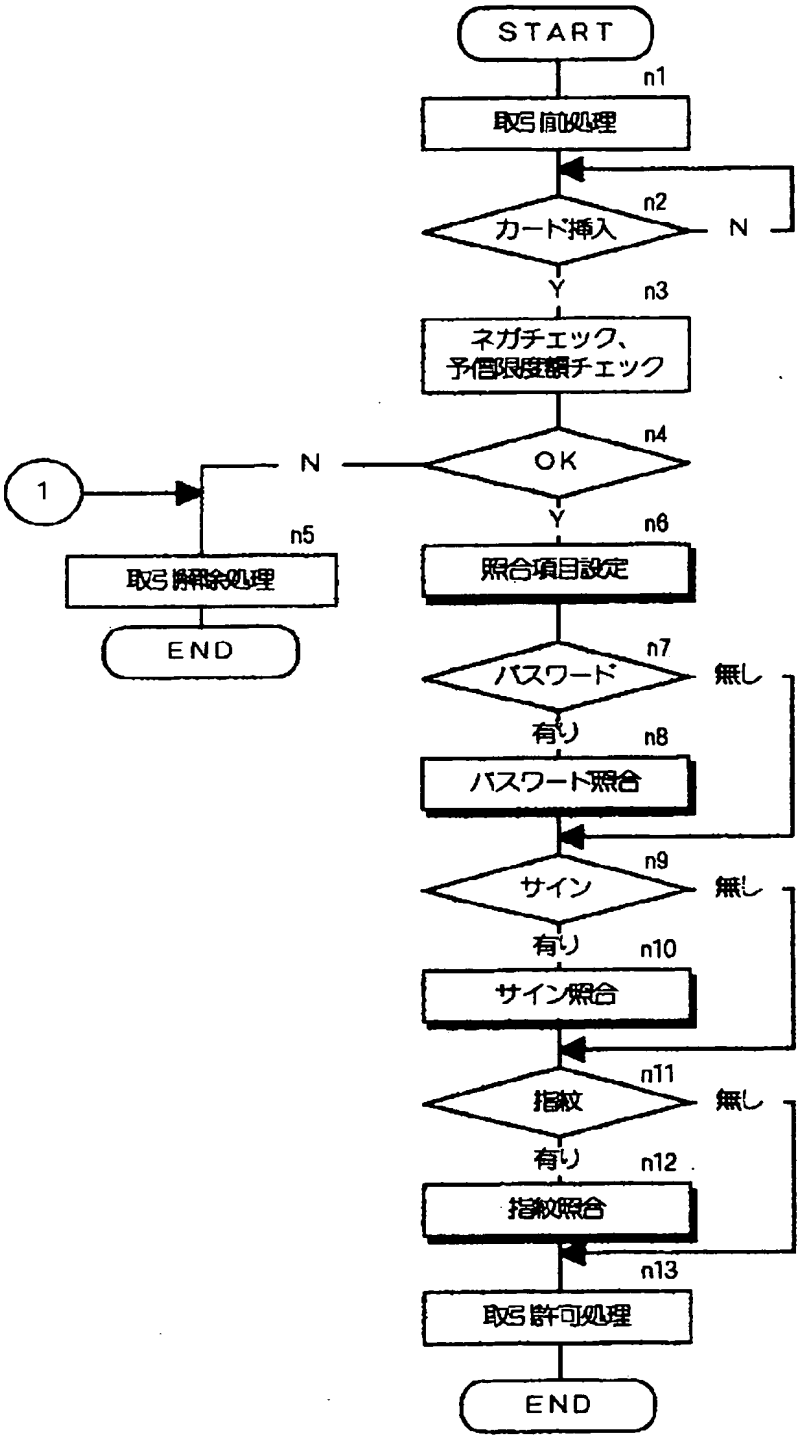
【図３】


2
3
4
5
6
7
ＩＣカード読取部
磁気カード読取部
キーパッド
タブレット
指紋読取機
25a
25b
25c
25d
25e
SW1
SW2
SW3
SW4
SW5
11
キーパネル
10
テンキーレス
CPU
21
24
選択条件入力設定部
26
ROM
RAM
モデム
22
23
ホストコンピュータ

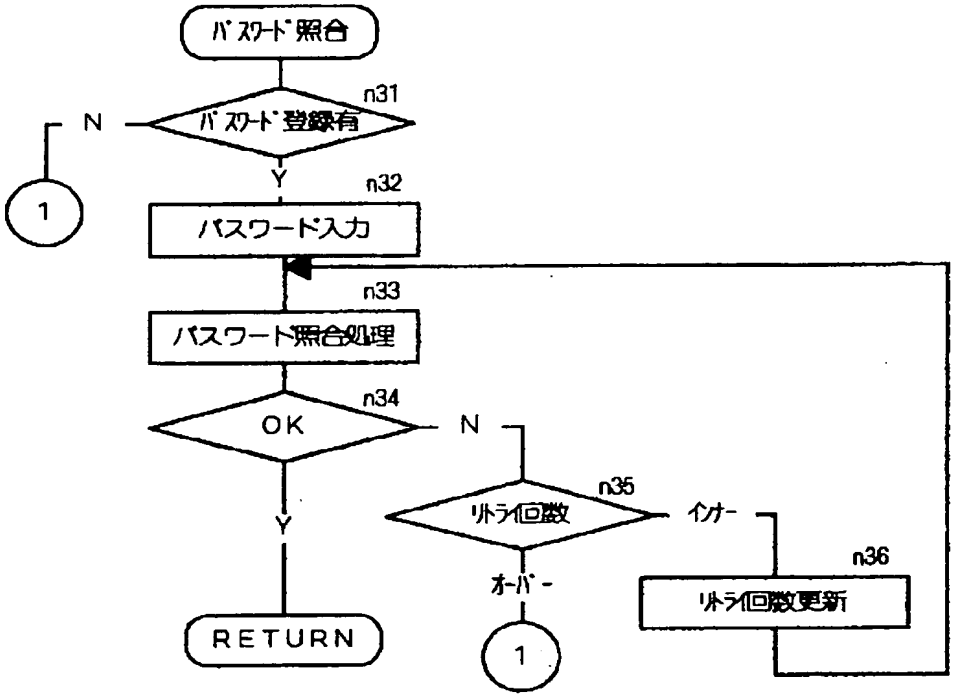
【図４】


電源オン
n51
初期化
n52
各入力装置検証
n53
各装置動作可
Y
N
n54
警告
n55
続行
N
Y
n56
所定時間
N
Y
n57
代用設定
n58
代用可能
N
Y
エラー処理
n59
各入力装置検証
n60
各装置動作可
N
Y
入力待ち

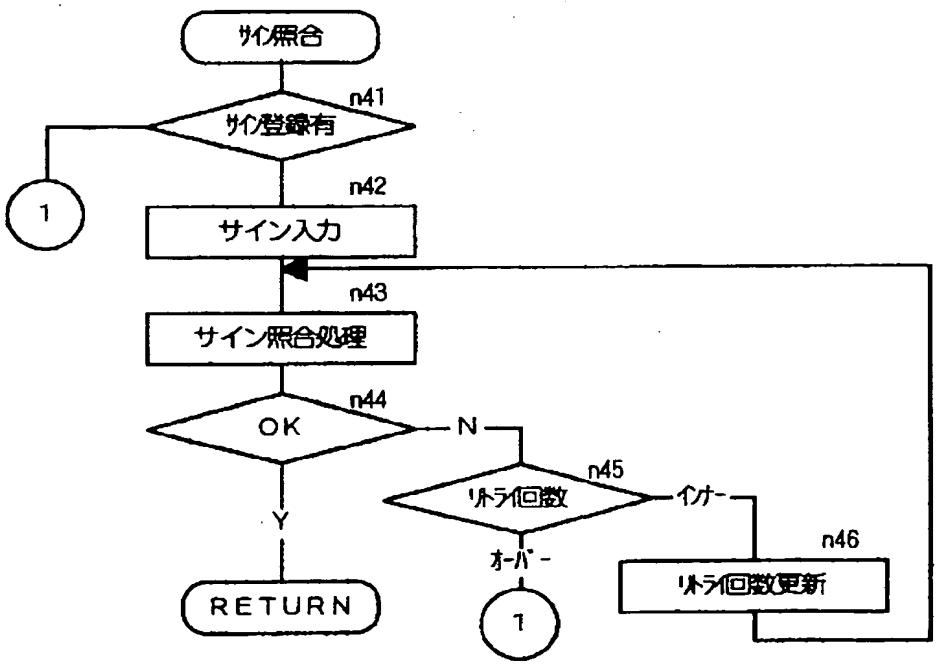
【図５】


START
n1
取引前処理
n2
カード挿入
N
Y
n3
ネガチェック、
予借限度額チェック
n4
OK
N
1
Y
n5
取引解除処理
END
n6
照合項目設定
n7
パスワード
無し
有り
n8
パスワード照合
n9
サイン
無し
有り
n10
サイン照合
n11
指紋
無し
有り
n12
指紋照合
n13
取引許可処理
END

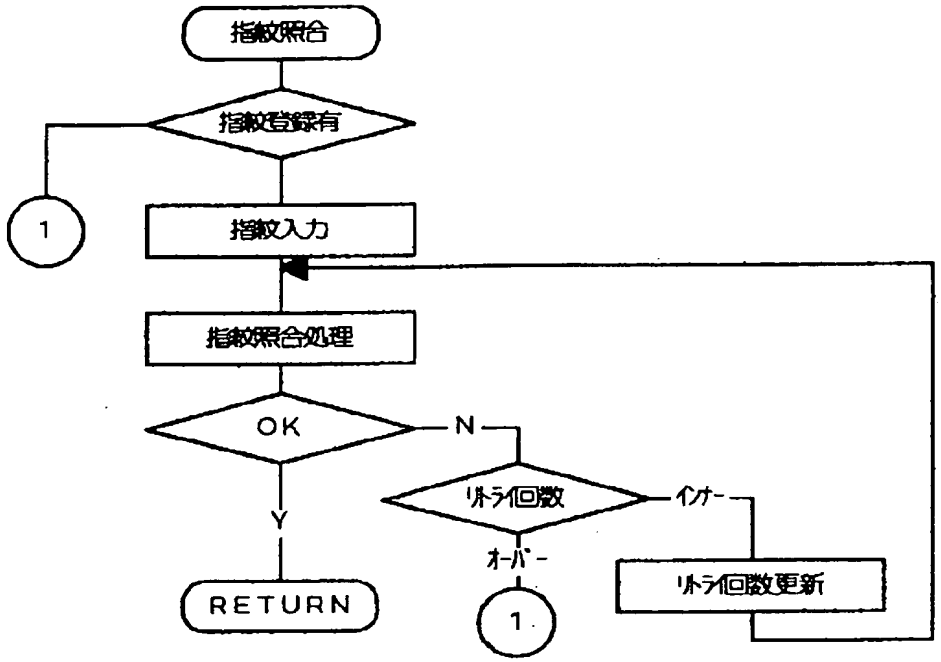
【図７】


ﾊﾟｽﾜｰﾄﾞ照合
n31
ﾊﾟｽﾜｰﾄﾞ登録有
N
Y
1
n32
パスワード入力
n33
パスワード照合処理
n34
OK
N
Y
RETURN
n35
ﾘﾄﾗｲ回数
ｵｰﾊﾞｰ
ｲﾝﾅｰ
1
n36
ﾘﾄﾗｲ回数更新

【図８】


ｻｲﾝ照合
n41
ｻｲﾝ登録有
1
n42
サイン入力
n43
サイン照合処理
n44
OK
N
Y
RETURN
n45
ﾘﾄﾗｲ回数
ｵｰﾊﾞｰ
ｲﾝﾅｰ
1
n46
ﾘﾄﾗｲ回数更新

【図９】


指紋照合
指紋登録有
1
指紋入力
指紋照合処理
OK
N
Y
リトライ回数
インナー
オーバー
RETURN
1
リトライ回数更新

JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11)Publication number: 07064911
(43)Date of publication of application: 10.03.1995

(51)Int.Cl.
G06F 15/00
G06F 19/00

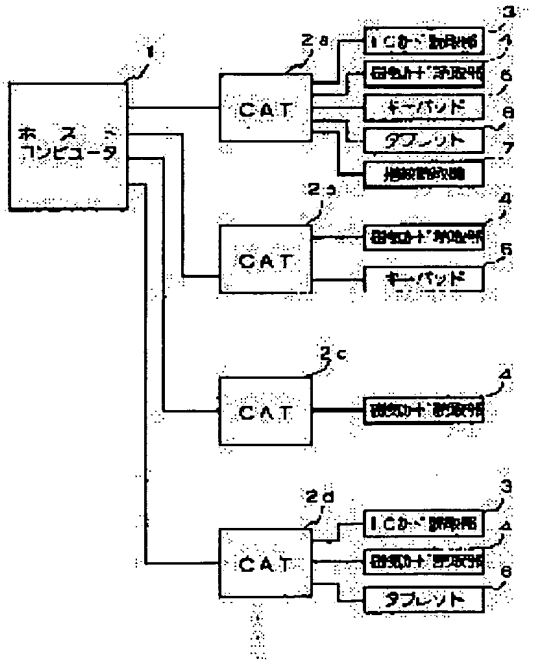
(21)Application number: 05216056
(22)Date of filing: 31.08.1993

(71)Applicant: SHARP CORP
(72)Inventor: ENOMOTO YOSHIHARU

(54) INDIVIDUAL AUTHENTICATION SYSTEM

(57)Abstract:

PURPOSE: To perform high-grade authentication and to improve security by connecting only the input devices of required items and authenticating individuals by the appropriately registered individual authentication data and the appropriately selected and connected input devices.
CONSTITUTION: In respective CAT terminals 2a, 2b..., an IC card read part 3 for inserting an IC card and reading the individual authentication data as the input device and a magnetic card read part 4 for reading the data of a magnetic card are provided at need and also a key pad 5 provided with keys for inputting a password, a tablet 6 for inputting a signature and a fingerprint reader 7 for inputting a fingerprint are connected at need. The individual authentication data for authenticating the individual and individual data such as an identification number or the like are stored respectively in the IC card and the magnetic card. The individual possesses either the IC card or the magnetic card at need and uses them appropriately in the view of a cost.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

HEI 7-64911

[CLAIMS]

[Claim 1]

Personal authentication system comprising:

personal data registering means for registering personal authentication data of desired number of items from the personal authentication data to identify a person such as password, handwriting and finger print or the like;

input device selecting means for selectively connecting the input devices of desired numbers from the input devices for inputting personal authentication data of each item; and

collating means for collating the personal authentication data input from said input device and the personal authentication data registered to said persoanl data registering means.

[Claim 2]

Personal authentication system as claimed in claim 1, characterized in comprising a collation item selecting means for selectively setting the collation items with said collecting means.

[Claim 3]

Personal authentication system as claimed in claim 2, characterized in comprising a means for alternately using the other items when the selected collation items cannot be used.

[0012]

It is therefore an object of the present invention to provide a personal authentication system which assures necessary checking to improve reliability of checking as required at each portion of the system.

[0019]

[Embodiment]

Fig. 1 is a diagram illustrating an example of structure of the personal authentication system in relation to the preferred embodiment of the present invention.

[0020]

A host computer 1 is connected with a plurality of CAT terminals 2a, 2b, ... Each CAT terminal 2a, 2b,... is provided, as required, with an IC card reading means 3 and a magnetic card reading means 4 to read data of a magnetic card to read the personal authentication data as an input device, a keypad (pin pad) 5 having the keys (ten keys for inputting password) for inputting the password, a tablet 6 for inputting a sign and a finger print reading device 7 for inputting finger print. The input device is enough when it allows input of data for authentication of a person and moreover a voice input device may also be connected to check voice print.

[0021]

In an IC card and a magnetic card to be inserted

to the IC card reading means 3 and magnetic card reading means 4, personal authentication data for authenticating person and personal data such as identification number are stored. To the IC card, the high-tech personal authentication data such as sign (handwriting) and finger print, etc. are also stored in addition to the ordinary data such as identification number, effective date and password or the like. Moreover, to the magnetic card, ordinary data, namely simple personal authentication data such as identification data, effective date and password is stored. Therefore, checking by collation of sign and finger print can be made to a person as a card holder in addition to the checking by the identification number and password. As a result, certainty of personal authentication can be improved.

[0022]

However, not only the IC card itself is expensive but also collation of sign and finger print require respective input devices, resulting in rise of cost. Meanwhile, certainty of personal authentication for a person as a card holder is not so high because only the check by identification number and password and visual check of sign are possible. In this case, however, the cost may be lowered.

[0023]

A person is caused to have, as required, any one of an IC card or magnetic card, but an IC card is used

when high level security is required or a magnetic card is used when ordinary security level is enough, considering the cost. For example, in case a card is designed as the financial dealing card such as a credit card, it can be thought that a customer who desires the dealing in a large amount of money has an IC card and a customer who desires only the dealing under the predetermined amount of money has a magnetic card. Moreover, in the case of checking of a person who is entering or going out of the room in a company, it is also though that a person who is entering or going out of a very important room has an IC card and a person who is entering or going out of an ordinary room has a magnetic card.

[0024]

In this embodiment, the personal authentication data is stored in the IC card and magnetic card but it is also possible to store such data in the CAT terminal 2 or host computer 1. When such data is stored in the host computer 1, collation can be made through communication between the CAT terminal 2 and host computer 1 at the time of collation. Namely, in above example, the personal data registering means is provided in the IC card or magnetic card, but such personal data registering means may be provided in the CAT terminal or host computer.

[0025]

As explained above, the CAT terminal 2a, 2b,.. respectively has, as required, an IC card reading means 3, a magnetic card reading means 4, a keypad 5, a tablet 6 and a data input device such as a finger print reading device 7, etc. Fig. 2 illustrates an example of structure of the CAT terminal and Fig. 3 is a block diagram of the CAR terminal.

[0026]

The CAT terminal 2 can be connected with the IC card reading means 3, magnetic card reading means 4, keypad 5, tablet 6 and input device such as finger print reading device 7, etc. via the switches SW1 to SW5 and connectors 25a to 25e. Therefore, only the necessary input devices may be connected using the connectors 25a to 25e. For example, in the case of the financial dealing system, the input devices to be connected can be set depending on the amount of money to be processed at the CAT terminal. For instance, in the case of the terminal for processing only a small amount of money, it is enough when only the magnetic card reading means 4 is provided for simplified checking and the keypad 5, etc. may also be added. Moreover, in the case of the terminal for processing a large amount of money, the IC card reading means 3, tablet 6 for collation of sign with higher certainty of personal authentication and finger print reading device 7 for collation of finger print may be added to perform the high level checking. Also, in the case of the system for

checking a person who is entering or going out of the room of a company, only the keypad 5 for inputting password or magnetic card reading means 4 is added when only the simplified check is necessary or these can be combined or the IC card reading means 3, tablet 6 and finger print reading device 7 for collation of sign and finger print may be provided when high level security is required. However, when personal data such as sign or finger print is stored in the IC card in such a condition that the tablet 6 for inputting sign and finger print reading device 7 for inputting finger print are connected, the IC card reading means 4 is the essential means.

[0027]

Moreover, the input device connected through the connectors can be validated or invalidated for the connecting condition by turning ON/OFF the switches SW1 to SW5. These switches SW1 to SW5 may be used for turning OFF an input device, for example, when such input device fails and for turning OFF an input device, for example, when an illegal act is found in such input device and collation by such input device is stopped. The connectors 25a to 25e and switches SW1 to SW5 correspond to the input device selecting means described in claim 1.

[0028]

Since the data input means can be set, as required, adequately for each CAT terminal as explained above, it

is no longer required to provide expensive devices such as IC card reading means 3, tablet 6 and finger print reading device 7 to the terminal which processes only the dealing in a small amount of money and thereby rise of cost more than that required for the system can be prevented. In addition, since personal check is possible using any one of the password, magnetic card and IC card, only a magnetic card is issued and issuance of expensive IC card may be avoided for the customer who requires, for example, only the dealing in a small amount of money. [0029]

The CAT terminal 2 comprises a CPU21 for controlling the processing operations of the CAT terminal and each input device connected to the CAT terminal, ROM 22 for storing the processing programs, RAM 23 for storing the selecting condition of each input device, selecting condition input setting means 24 for inputting each input device selecting condition, modem 26 for communication with the host computer 1, display 10 and key panel 11 for inputting amount of money for dealing or the like. The selecting condition input setting means 24 and selecting condition storing means of RAM 23 correspond to the collation item selecting means described in the claim 2. [0030]

The selecting condition input setting means 24 is used for inputting the selecting conditions of the input device, for example, at the time of setting the terminal

and conducting the maintenance as required. For example, in the financial dealing device, the personal authentication method is set and input for each input amount of money and the personal authentication method is set and input depending on the place where the CAT terminal is installed. Moreover, for example, in the case of checking for a person who is entering or going out of a room, personal authentication method is set depending on a degree of importance. At the time of input, alternating sequence of each input device is also input simultaneously from the selecting condition input setting means 24. For example, if the IC card reading means is disabled for use, an alternate authentication method is input in order to alternately use the magnetic card reading means. In this case, the personal authentication process is executed depending on the preset selecting condition.

Fig. 1:

1: Host computer; 3: IC card reading means;

4: Magnetic card reading means; 5: Keypad;

6: Tablet; 7: Finger print reading device;

Fig. 3:

Host computer;

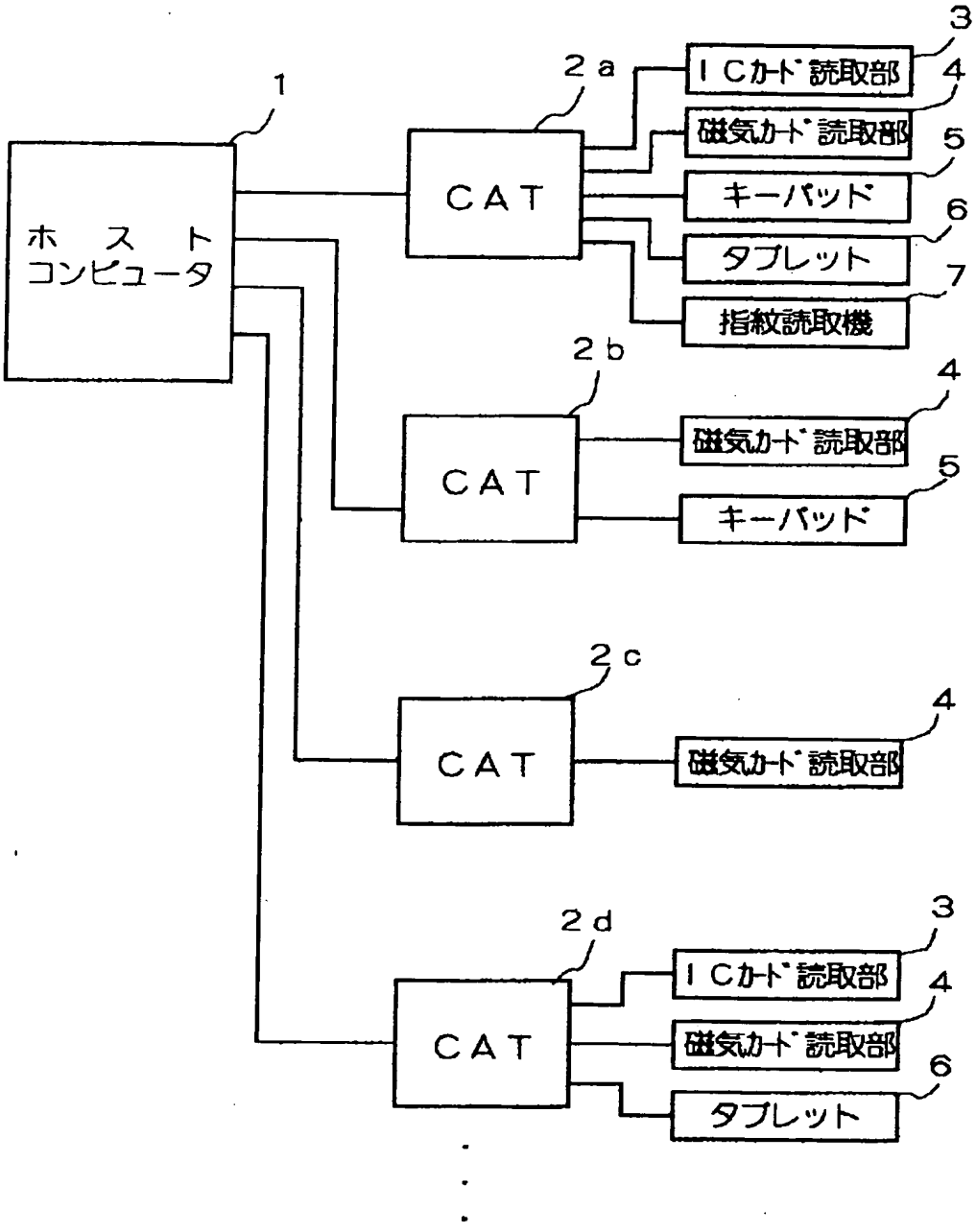
3: IC card reading means; 4: Magnetic card reading means;

5: Keypad; 6: Tablet; 7: Finger print reading device;

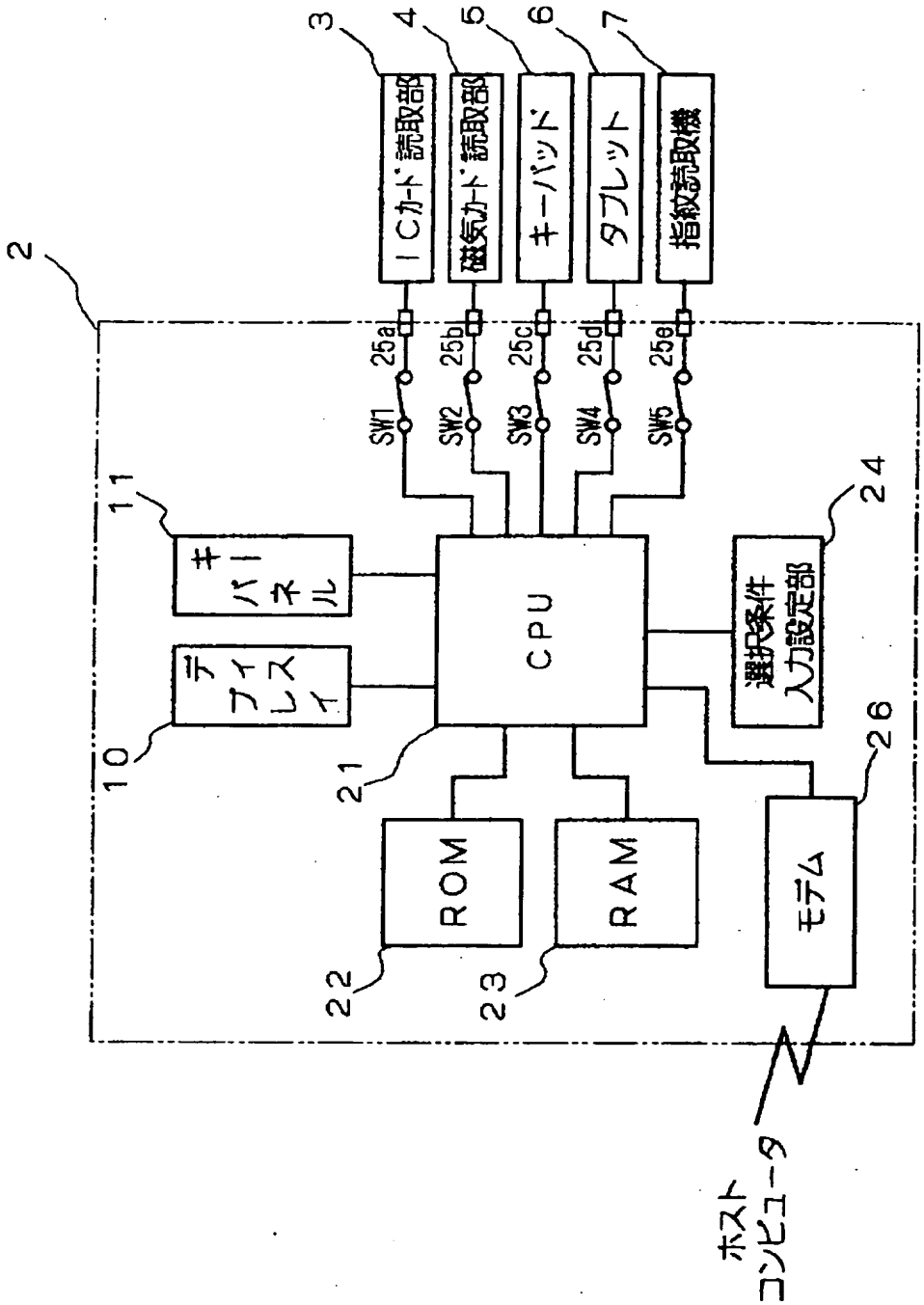
10: Display; 11: Key panel;

24: Selecting condition input setting means;

【図1】 Figure 1


1
ホスト
コンピュータ
2a
CAT
3
ICカード読取部
4
磁気カード読取部
5
キーパッド
6
タブレット
7
指紋読取機
2b
CAT
4
磁気カード読取部
5
キーパッド
2c
CAT
4
磁気カード読取部
2d
CAT
3
ICカード読取部
4
磁気カード読取部
6
タブレット

【図3】 Figure 3


2
3
4
5
6
7
ICカード読取部
磁気カード読取部
キーパッド
タブレット
指紋読取機
25a
25b
25c
25d
25e
SW1
SW2
SW3
SW4
SW5
11
キーパネル
10
ディスプレイ
CPU
21
24
選択条件入力設定部
26
ROM
RAM
モデム
22
23
ホストコンピュータ